Remarks

In view of the above amendments and the following remarks, reconsideration of the rejection and further examination are requested.

Claims 23 and 32 have been cancelled without prejudice or disclaimer to the subject matter contained therein.

Claims 19-42 have been rejected under 35 U.S.C. §103(a) as being unpatentable over Sims III (US 2002/0016919) in view of Admitted Prior Art (APA) and Oshima (US 7,191,154).

Claims 19, 28 and 37 have been amended so as to further distinguish the present invention, as recited therein, from the references relied upon in the rejection.

It is submitted that the above-mentioned rejection is inapplicable to the amended claims for the following reasons.

Claim 19 is patentable over the combination of Sims III, APA and Oshima, since claim 19 recites a playback terminal including, in part:

a medium content key calculation unit operable to cryptographically calculate a medium content key using medium information and information pre-stored in the playback terminal itself;

a license content key calculation unit operable to cryptographically calculate a license content key using the medium content key and managed information acquired from an external license server; and

a decryption unit operable to (a) decrypt the encrypted content using the medium content key, when it is judged that the managed information is not required, and (b) decrypt the encrypted content using the license content key, when it is judged that the managed information is required.

With the above features, the invention as recited in claim 19 has a number of advantages over other systems.

A first advantage is that it is possible to appropriately decrypt encrypted content regardless of whether the encrypted content is protected with a first protection method or a second protection method. When the first protection method is used, the encrypted content cannot be decrypted unless managed information (e.g., rights information) is acquired from an external license server via a network. On the other hand, when the second protection method (e.g., Contents Scrambling System (CSS) for Digital Versatile Discs (DVDs)) is used, the

encrypted content is decrypted using medium information pre-recorded on the portable medium without a network connection.

A second advantage is that the managed information acquired from the external license server is not a decryption key per se that is used for the decryption of the encrypted content. Therefore, even if the managed information is stolen by an unauthorized person on the communication path between the playback terminal and the external license server, the encrypted content cannot be decrypted with only the stolen information. This prevents the unauthorized use of the content.

A third advantage is that regardless of whether the managed information is (i) required (i.e., the first protection method) or (ii) not required (i.e., the second protection method), it is not necessary to prepare two different key generation units for the first and second protection methods, since the medium content key calculated by the medium content key calculation unit is used to decrypt the encrypted content in both the first and second methods.

It is submitted that the combination of Sims III, APA and Oshima fails to disclose or suggest the above features of claim 19, and therefore, cannot achieve the advantageous effects of the present invention as recited therein.

Sims III discloses an invention relating to the use of encrypted content stored on a recording medium. In the system of Sims III, there is a first case in which encrypted content stored on the recording medium is decrypted using information stored on a recording medium, and a second case in which information is acquired from an external server and the encrypted content stored on the recording medium is decrypted using the acquired information. (See paragraphs [0087] and [0088]).

Sims III discloses that if information from an external source is to be required in order to utilize the content of media 100, the operation of the system proceeds to step 211 wherein a content key is selected at random, or by another appropriate method. The content key of step 211 is provided to a clearing house, or another external agent, in order to provide for the later use of the content of the media 100. Sims III also discloses that the content key is not stored on media 100, thus requiring contact with the clearing house for use of the content. Further, Sims III discloses that regardless of whether or not an external source is to be utilized, the content to be stored within an unsecured area 102 on the media 100 may be encrypted with the content key (step 213) and recorded to the media 100 (step 214). (See paragraphs [0088] and [0089]).

Based on the above discussion, it is apparent that the system of Sims III is such that when the encrypted content is encrypted with the content key and information from the clearing house is required to decrypt the encrypted content, the content key itself is transmitted from the external server to the player. Therefore, with the system of Sims III, the content would be able to be decrypted without authorization by a third party who steals the content key during transmission on the communication path between the player and the external server.

In contrast, as discussed above, the playback terminal as recited in claim 19 has the aforementioned feature that the encrypted content cannot be decrypted using only the managed information acquired from the license server, and to decrypt the encrypted content, the medium information and the information pre-stored in the playback terminal are required in addition to the managed information acquired from the license server. This feature is set forth in the claimed license content key calculation unit which is operable to cryptographically calculate a license content key using the medium content key and managed information acquired from an external license server. Due to this feature, the playback terminal of claim 19 has the added benefit of preventing malicious decrypting of the content if the managed information managed by the external license server is stolen by a third party during transmission over the transmission path between the playback terminal and the license server. This benefit is not realized with the invention of Sims III. As a result, APA and/or Oshima must disclose or suggest this feature of claim 19.

Regarding APA, it is relied upon as disclosing the use of information stored in a playback terminal for generating a content key. However, APA also fails to disclose or suggest the above-discussed feature of claim 19. Therefore, Oshima must disclose or suggest this feature in order for the combination of Sims III, APA and Oshima to render claim 19 obvious.

Oshima discloses a system for encrypting and decrypting information stored on a removable disk. When encrypted content (i.e., '1-n'th content) located on a removable disk is to be decrypted for playback with a first computer 909, a password generation part 834, which includes an operation expression of public cipher keys, in a password issue center (i.e., second computer) 821 generates a password (i.e., '1-n'th password) by enciphering three data fields with a public key. The three data fields are a disk ID, a content number of the encrypted content (i.e., the content that a user wishes to unlatch), and time data representing the period that use of the content is allowed. The generated password 843a is then sent to the first computer 909.

The first computer 909 receives the password 843a and decodes it with a secret key corresponding to the public key. The resultant information is the mixed keys of the disk ID, the timing data and the content number. A password checking part 836 in the first computer 909 checks the ID 835a of the BCA reproduced from the disk, the present second timing data 835b, the allowed ID 833a and the first timing data 833, and determines whether they coincide. If the information coincides, it is allowed and the decoding key 836a (i.e., '1-n'th decoding key) is output to a cipher decoder 837. The cipher 837a of the '1-n'th content is then decoded and the 'n-1'th content 838 is output. (See column 6, lines 42-67 and Figure 6).

Based on the above discussion, it is apparent that the system of Oshima is such that the first computer 909 decodes the encrypted content from the disk based on a decoding key pre-recorded on the disk. However, before the first computer 909 can use the pre-stored decoding key, the password acquired from the password issue center 821 is used to verify the time data and the decoding of the decoding key which has been enciphered. Therefore, it can be said that the system of Oshima is somewhat similar to the present invention in the sense that enciphered content cannot be decoded solely with the information acquired from the password issue center 821.

However, it is also clear that the system of Oshima is different from the present invention as recited in claim 19 in that Oshima fails to disclose or suggest either the claimed medium content key calculation unit operable to cryptographically calculate a medium content key using medium information and information pre-stored in the playback terminal itself, or the claimed license content key calculation unit operable to cryptographically calculate a license content key using the medium content key and managed information acquired from an external license server. Therefore, Oshima fails to address the deficiencies of Sims III and APA. As a result, claim 19 is patentable over the combination of Sims III, APA and Oshima.

As for claim 28 and 37, they are patentable over the combination of Sims III, APA and Oshima for reasons similar to those discussed above in support of claim 19.

Because of the above-mentioned distinctions, it is believed clear that claims 19-22, 24-31 and 33-42 are allowable over the references relied upon in the rejection. Furthermore, it is submitted that the distinctions are such that a person having ordinary skill in the art at the time of invention would not have been motivated to make any combination of the references of record in such a manner as to result in, or otherwise render obvious, the present invention as recited in

claims 19-22, 24-31 and 33-42. Therefore, it is submitted that claims 19-22, 24-31 and 33-42 are clearly allowable over the prior art of record.

In view of the above amendments and remarks, it is submitted that the present application is now in condition for allowance. The Examiner is invited to contact the undersigned by telephone if it is felt that there are issues remaining which must be resolved before allowance of the application.

Respectfully submitted,

Masaya YAMAMOTO et al.

By: /David M. Ovedovitz/
2009.08.24 10:28:01 -04'00'

David M. Ovedovitz
Registration No. 45,336
Attorney for Applicants

DMO/jmj
Washington, D.C. 20006-1021
Telephone (202) 721-8200
Facsimile (202) 721-8250
August 24, 2009